PATENT SPECIFICATION (11) 1 499 974

1 499 974

(21) Application No. 53915/71 (22) Filed 19 Nov. 1971
(31) Convention Application No. 2058796
(32) Filed 30 Nov. 1970 in
(33) Federal Republic of Germany (DE)
(44) Complete Specification published 1 Feb. 1978
(51) INT CL² H04L 9/00
(52) Index at acceptance
H4P B1 B2 B6A B6Y E9 S2
G4D 6C1 6Y 7G

(19)

(54) SYNCHRONIZING RANDOM-CHARACTER GENERATORS OF A SECURE MESSAGE TRANSMISSION SYSTEM

(71) We, LICENTIA PATENT-VERWALTUNGS-G.M.B.H., of Theodor-Stern-Kai, 6 Frankfurt 70, Federal Republic of Germany, a German Body Corporate, do hereby declare the invention, for which we pray that a patent may be granted to us, and the method by which it is to be performed, to be particularly described in and by the following statement:—

The invention relates to a secure message transmission system, and to a method for synchronising the random-character generators which are arranged at the sending and receiving ends of the transmission path.

In order to transmit coded (ciphered) messages, it is known for the clear-text characters to be combined at the sending end in some way or another, for example by mod-2 addition, with cipher characters obtained from a so-called random character generator, in order to obtain ciphered characters for transmission. At the receiving end, the ciphered characters must be converted back again into the clear-text characters by corresponding combination, e.g. a further mod-2 addition, with the same cipher characters. Whatever may be the rule according to which the ciphered characters are formed from the clear-text characters and the cipher characters, it is necessary in any case to ensure that the random-character generators at the sending and receiving ends run synchronously. For this purpose, it has been the practice to cause the random character generators to be brought repeatedly into their agreed initial settings in order to restore the synchronism which may in certain circumstances have meanwhile been lost. Since this resetting involves repetition of the same sequence of random characters, cryptological security is prejudiced.

In order not to use the same sequence of random characters again each time operation is resumed, and thus in certain circumstances produce "passages in the same phase", a basic key held by both sending and receiving ends which determines the initial setting may be supplemented by an additional key capable of being varied each time operation is started. This variable additional key is for example produced by the random-character generator in the transmitter, and transmitted to the receiving end in uncoded form as a block of characters. In that case an unauthorised decipher may therefore acquire a knowledge of part of the setting key being used, with the result that, for a simple ciphering process, he is able in certain circumstances, and with the aid of the ciphered text, to draw conclusions regarding the basic key and thus to decode messages being transmitted. Clearly the risk of code-recognition increases with the number of times the random-character generators are reset to their initial state. The risk increases still further if the number of definite initial settings of the random-character generators has to be increased in order to enable further receivers to be switched into message-transmissions already in progress. This very greatly reduces cryptological security, the more so since the variable additional key continuously varying the initial settings allows of only a limited number of possible variations, while a substantial part of the code setting, the so-called basic key, remains unaltered.

One common form of so-called random character generator comprises a plurality of cyclical counters, each having a capacity P which is a prime number, preferably different from the other counters. If all the counters are stepped on in synchronism from their zero settings, each will reach its capacity and re-set at different times, and therefore the sequence of numbers formed by the instantaneous count M in each of the counters will have a pseudo-random

distribution. The length of the sequence before it repeats is of course determined by the number of counters used and their capacities, but is stretched to the maximum when the capacities are primes.

In order to be able to produce different sequences it is normal to use a basic key consisting of a set of initial settings G for each counter. The basic key, or a number of alternative basic keys, are held as secret information at both sending and receiving ends.

Now if the total number of timing pulses A by which a counter has been switched onwards starting from its initial setting G is known, it is possible to calculate the instantaneous value M of the counter. Dividing

$$\frac{\text{total number of timing pulses A}}{\text{prime number capacity P of counter}} = \text{N+remainder X}$$

where the integral value N represents the number of cycles of the counter which have been run through, and the remainder value X giving the count of timing pulses of a cycle started from G. This calculation can be carried out for each individual counter of the random-character generator. The number N of complete cycles of the relevant counter which have been run through starting from the initial value G is not necessary in order to determine the actual instantaneous state M of the counter, since the latter can be unambiguously determined by adding the initial value G and the remainder value X:

$$M=G+X,$$

the modulus of addition being the relevant prime number P.

Now the invention is based on the fact that only if both the terms G and X of each counter of the random-character generator at the sending end are known can a similar random-character generator at the receiving end be brought into synchronism. With the usual and necessary agreement of the basic key giving the value G for each counter, transmission of the value X alone to the receiving end can enable synchronisation at the sending end, but now without any loss of cryptological security.

The invention therefore proposes a method of synchronising the random character generators at the sending and receiving ends of a secure message transmission system, wherein each generator includes a plurality of cyclicial counters with prime number capacities, and the random characters for ciphering and deciphering are produced by use of identical basic keys representing initial settings of counters, which method comprises: transmitting to the receiving end data identifying the count reached by each counter independently of said initial setting, and comparing the data with the count reached by each counter at the receiving end.

One possibility is that each counter is initially set by said basic key and is then stepped on by clock pulses such that its instantaneous state forms an element of a random character, said data for each counter at that instant being obtained by division of the total number of steps of the counter by its respective prime number capacity to give a dividend (which is neglected) and a remainder which forms said data.

Another possibility is that said cyclical counters are initially set at zero and are stepped on by clock pulses, the instantaneous state of said cyclical counters forming said data, and the random characters being formed by using the result of the addition of said data to said initial settings.

In a preferred form of the invention, the latter method is modified by arranging that each counter at the transmitting end, or at both the transmitting and receiving ends, is associated with a further counter which is initially set by said basic key and stepped on simultaneously by said clock pulses, such that its instantaneous state forms an element of a random character. The synchronising data may be inserted at fixed or variable time-intervals into the coded message-transmission. In order to make it easier for a non-synchronous receiver which is picking up these messages to recognise the inserted synchronising data, in the form of the values X, it is expedient to characterise their transmission by an agreed code-word.

When the method according to the invention is used, synchronism, once it has been obtained, can be continuously checked by comparing the instantaneous values X communicated from the sending end and of the instantaneous values X' derived at the receiving end, which values are identical if synchronism exists.

When synchronisation has been achieved, a receiver is not obliged, in spite of the repeated possibility of synchronising and by contrast with known processes, to make further adjustments to the counters of its random-character generator which might in some circumstances involve a loss of its synchronism due to errors in

transmission, since neither does the random-character generator at the sending end make any new adjustments to its counters while a message is being transmitted.

An exemplary embodiment of the invention will be more precisely explained hereinafter, with reference to the drawings, in which:

Figure 1 shows a summary block circuit diagram of a system for the ciphered transmission of binary-coded messages, and

Figures 2 shows random character generators at the sending and receiving ends of the system.

In Figure 1, the clear text KT to be encoded is fed at the sending end via the line 1 to a coding appliance 2 in which it is encoded by combination with cipher characters ST and by computing operations of any desired kind to form the ciphered text GT which is fed to the transmission line 7. The cipher characters ST are produced in a random-character generator 4 the construction of which is more precisely explained below with reference to Figure 2. At the receiving end, there is a decoding appliance 10 in which the received ciphered text GT is decoded to form the clear text by computing operations with the identical cipher characters ST produced in a random-character generator 12 similar to generator 4.

In the simplest case, encoding is carried out simply by mod-2 addition of the clear-text bits to cipher characters, and decoding is then carried out by further mod-2 addition of the same cipher characters to the transmitted ciphered text. However, the invention is not limited to the use with such a simple encoding system, but may also be used in conjunction with any other ciphering systems which work with quasi-random-character generators running synchronously.

Introduction of the remainder values X (SX) as previously discussed into the transmitting line 7 is effected by the switch 5 and via the line 6. They are extracted and fed to the random-character generator 12 at the receiving end by the switch 8 and via the line 9.

The invention may likewise also be used in conjunction with random-character generators which serve other purposes, such as producing sequences involving a sudden change in frequency or spread codes, without coding appliances 2 and 10.

Figure 2 shows the random character generators for a system as illustrated in Figure 1. The random character generators at the sending and receiving ends to which the invention may be applied are represented by ZG1 and ZG2. In each case there are n counters Z1, Z2.... Zn and Z1'.... Zn' with prime number counting bases, only three, 28, 29 and 30, and 44, 45 and 46, being illustrated in each case. These counters are stepped on one step at a time by timing pulses from a timing-pulse source 31 or 47, and each, for example upon reaching its maximum state, passes on an output pulse to a compiler 32 or 48 in which the random characters ST are produced by processing the output signals of the counters which arrive at irregular intervals.

Back-coupled shift-registers may alternatively be used to fulfil the functions of the counters Z1 ... Zn or Z1'.... Zn'. The back-coupling in such shift-registers may be so adjusted that the cycles repeat themselves after a prime number of steps. When reference is made herein to counters this is always to be understood to include shift-registers.

Each counter Z1 ... Zn or Z1' ... Zn' has associated with it a register 22, 23, 24 or 38, 39, 40, which contains part of the basic key settings G1 .... Gn or G1' .... Gn' for the counters.

In addition, counting registers 19, 20, 21 or 35, 36, 37, are provided each likewise associated with a counter Z1 ... Zn or Z1'.... Zn'. The counting bases or capacities of the counters 19, 20, 21 or 35, 36, 37 are likewise prime numbers, and correspond to those of the counters Z1 ... Zn or Z1'.... Zn' with which they are associated. Sum-formation takes place in addition circuits 25, 26, 27 or 41, 42, 43, to give the same values M1—Mn or M1'—Mn' as the counters 28, 29, 30 or 44, 45, 46. The counters 28, 29, 30 or 44, 45, 46 at the sending and receiving ends are simultaneously adjusted to the initial setting determined by the basic key held in counters 22 ...., 38 .... This means that at both ends and in all counters the terms X=0. The counting registers 28, 29, 30 or 44, 45, 46, and 19, 20, 21, or 35, 36, 37, are thereafter synchronously switched onwards by the timing generators 31 or 47. The registers 19, 20, 21 or 35, 36, 37 thus contain at any instant the values X1 ... Xn or X1' ... Xn', which when added (on the relevant prime number base) to the values G1 ... Gn or G1' ... Gn', give the instantaneous values M1 ... Mn or M1' ... Mn' of the counters Z1 ... Zn or Z1' ... Zn' (e.g. Mi=Gi+Xi).

If for any reason the random-character generator ZG2 at the receiving end now drops out of synchronisim, the contents of the registers 35, 36, 37 can first of all be brought into synchronism with the sending end by comparing the values X1 ... Xn of the register-contents 19, 20, 21 transmitted over the line 49. The subsequent additions (X1' ... Xn+G1' ... Gn') modulo P1' ... Pn' in the addition circuits 41, 42, 43

to give M1′ ... Mn′, and the transfer of the result of the registers 44, 45, 46 effects the desired synchronisation of the counters Z1′ ... Zn′ of the random-character generator ZG2 at the receiving end.

Although the embodiment of Figure 2 is preferred it is clear that counters 28, 29, 30 and counting registers 19, 20, 21 are holding duplicated information, since the contents of the former are in each case merely the sums of the contents of the latter with a constant (the values G1 ... Gn held by registers 22, 23, 24). Thus one or other may if desired be dispensed with, and the values X or M simply derived respectively from M or X, whichever is present. M is formed by simple addition G+X; X is formed by division A/P=N+X, as explained above.

WHAT WE CLAIM IS:—

1. A method of synchronising the random-character generators at the sending and receiving ends of a secure message transmission system, wherein each generator includes a plurality of cyclical counters with prime number capacities, and the random characters for ciphering and deciphering are produced by use of identical basic keys representing initial settings of counters which method comprises: transmitting to the receiving end data identifying the count reached by each counter independently of said initial setting, and comparing the data with the count reached by each counter at the receiving end.

2. A method as claimed in claim 1, wherein each counter is initially set by said basic key and is then stepped on by clock pulses, such that its instantaneous state forms an element of a random character, said data for each counter at that instant being obtained by division of the total number of steps of the counter by its respective prime number capacity to give a dividend (which is neglected) and a remainder which forms said data.

3. A method as claimed in claim 1, wherein said cyclical counters are initially set at zero and are stepped on by clock pulses, the instantaneous state of said cyclical counters forming said data, and the random characters being formed by using the result of the addition of said data to said initial settings.

4. A method as claimed in claim 3, wherein each counter at the transmitting end, or at both the transmitting and receiving ends, is associated with a further counter which is initially set by said basic key and stepped on simultaneously by said clock pulses, such that its instantaneous state forms an element of a random character.

5. A secure message transmission system when used in carrying out the method of any one of claims 1 to 4.

6. A method of synchronising random character generators substantially as herein described with reference to the drawings.

7. A secure message transmission system substantially as herein described with reference to the drawings.

For the Applicants:
J. F. WILLIAMS & CO.,
Chartered Patent Agents,
113 Kingsway,
London WC2B 6QP.

Printed for Her Majesty's Stationery Office, by the Courier Press, Leamington Spa, 1978
Published by The Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.

1499974 COMPLETE SPECIFICATION
2 SHEETS This drawing is a reproduction of the Original on a reduced scale
Sheet 1

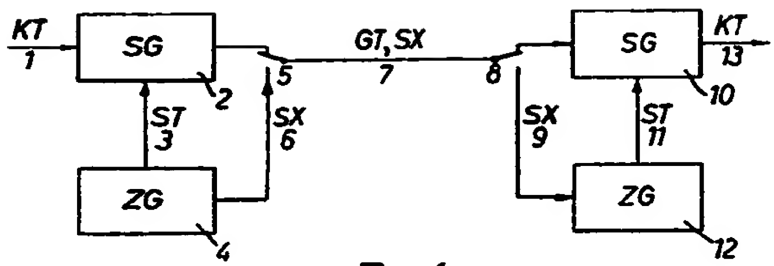

FIG. 1

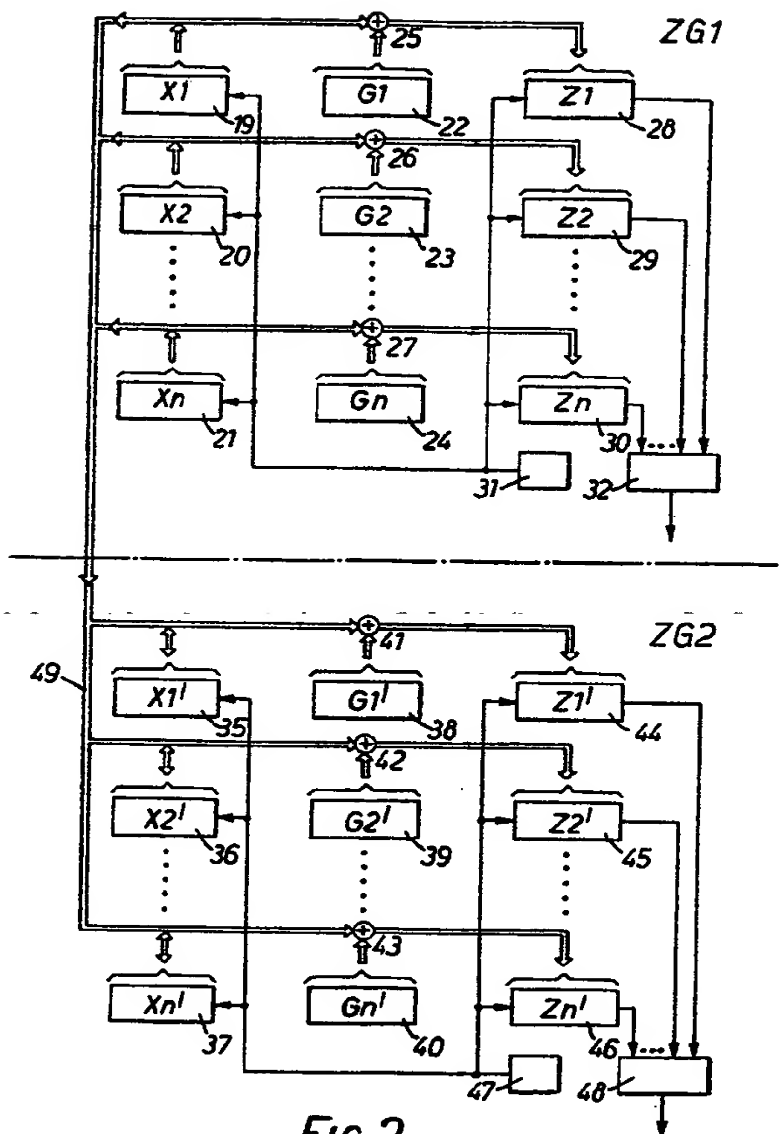
ZG1
X1
G1
Z1
X2
G2
Z2
Xn
Gn
Zn
ZG2
X1'
G1'
Z1'
X2'
G2'
Z2'
Xn'
Gn'
Zn'
19
20
21
22
23
24
25
26
27
28
29
30
31
32
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49

FIG. 2

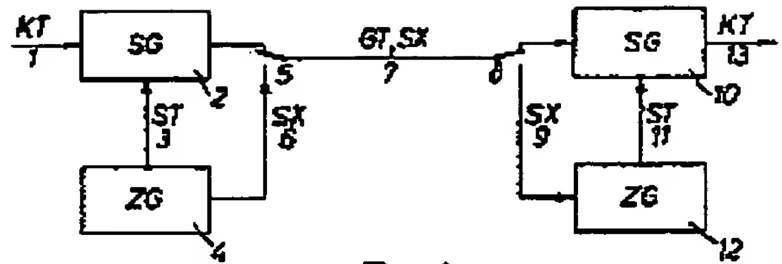

FIG. 1

1499974 COMPLETE SPECIFICATION
2 SHEETS This drawing is a reproduction of the Original on a reduced scale
Sheet 2

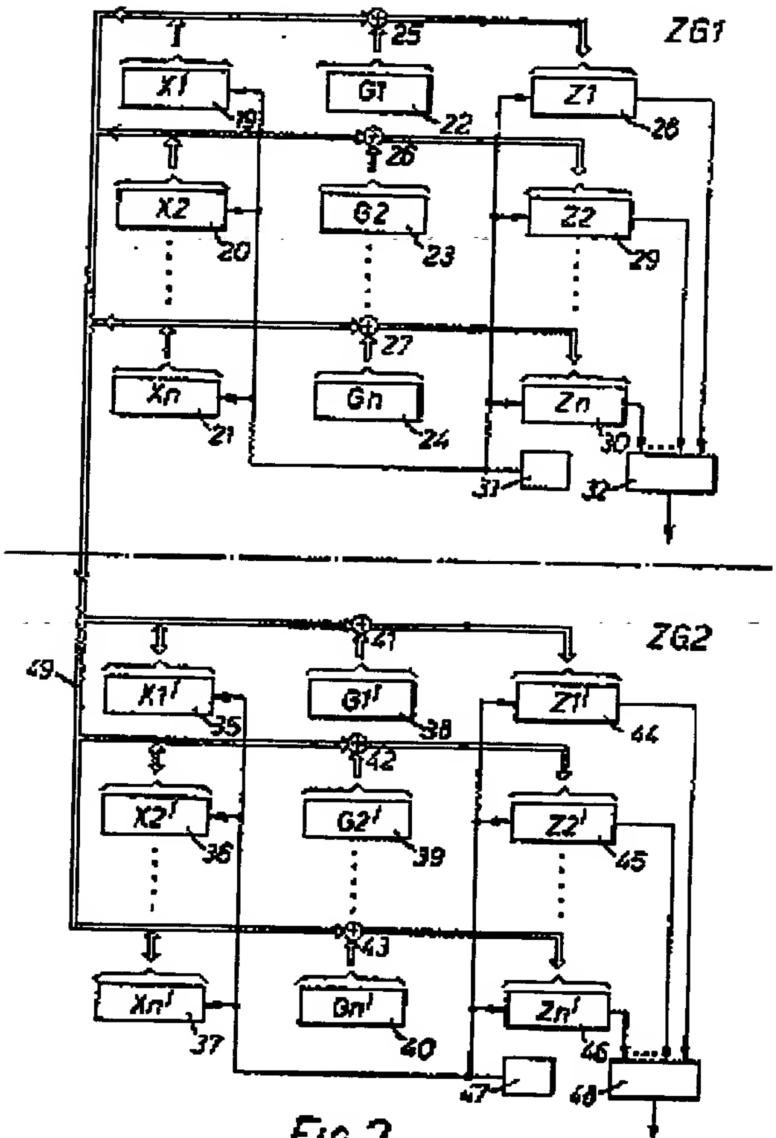

FIG. 2